UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,820	10/31/2001	Richard Paul Tarquini	10017334-1	4709

7590 10/24/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 10/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/003,820	**Applicant(s)** TARQUINI ET AL.	
	Examiner Carl Colin	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _07 August 2006_.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-20_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-20_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 8/7/2006, applicant amends claims 1, 2, and 13, and adds claims 18-20. The following claims 1-20 are pending and are presented for examination.

1.1 Applicant's arguments, pages 6-13, filed on 8/7/2006, with respect to the rejection of claims 1-17, have been fully considered, but they are not persuasive. Regarding claim 1, Applicant states that Taylor does not disclose the configuration file comprises at least one field that includes information from which a determination is made as to whether an intrusion protection evaluates the network exploit rule as amended because Taylor appears to teach that all rules are all evaluated. Examiner respectfully disagrees. Taylor discloses that the proxy determines which filter rule to apply. Taylor also discloses selective filter rule to be applied for specific connections as shown below:

> "Proxy 211, upon receiving the attribute information from DPF 207, determines whether to allow the connection." (col. 6, lines 21-25).
>
> "Another dynamic filter rule is a selective filtering rule. This rule requires proxy 211 to handle connection control packets and packet filters to handle the data packets. In other words, the packet filtering will be enabled only when proxy 211 has performed it's security checks for the connections, i.e., checking the relevant information on the SYN packet sent by DPF 207. For instance, this rule is useful for protocols such as File Transfer Protocol (FTP), which sends data packets on a different connection after establishing the connection. Other filtering rules are also possible such as not applying any filtering or applying a proxy filter at the application layer to all packets received on a specific connection.
>
> The configuration file discussed above, which stored the information on which ports are registered, further includes various filter rules to be applied for specific connections. For example, packets received from a particular port can be subjected to the filter all rule filter, while packets

received from another port can be subjected to the selective filtering rule." (col. 6, lines 30-50).

"Once proxy 211 determines whether to allow the connection and which one of the rules to apply to the connection, that information is transferred to DPF 207." (col. 6, lines 58-60).

Applicant adds that Taylor does not disclose an Enabled field value or a Severity field value. Examiner respectfully disagrees. The "allow/deny" field specifies the port to be filtered during generation of the text file that meets the recitation of enabled field value. Taylor also specifies a filter rule with the range of ports to be allow or deny that also meets the recitation of severity field value as shown by Applicant's response on page 10. Taylor even discloses field value indicating type of filter rule to apply that meets the recitation of enabled field value and/or severity field value in the citation provided by Applicant's response on page 10. Regarding claim 13, Applicant argues that Taylor does not disclose compiling input into a machine readable signature file comprises a network rule. Examiner respectfully disagrees. Applicant's citation on page 9 of the response explicitly recites, the rules may be entered by Administrator. In addition, Taylor also discloses,

"In order to determine whether to allow the requested data communication connection, the proxy compares the attribute information with rules in configuration information file. The rules in the configuration information file are entered by a user to set forth whether to allow data communication connections for certain physical connections. If the rule is to allow the data communication connection and forward the packets at the packet level, the dynamic packet filter creates a connection rule so as to apply the connection rule to packets having the same attribute information. Subsequent packets received with the same attribute information are then automatically forwarded without consulting the proxy. Once the connection terminates, the connection rule is removed and the proxy is notified. However, if the decision is to absorb, the dynamic packet filter sends the packets up a TCP/IP stack in the firewall, where they will be accepted by the proxy." (col. 3, line 54 - col.4, line 3).

As shown above, applicant has not overcome the rejection. The added limitations are further disclosed in view of the same references, Taylor and Freund, as shown in the rejection below.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2.1 Claim 1 and the intervening claims are rejected under 35 U.S.C. 112, second paragraph, as failing to set forth the subject matter which applicant(s) regard as their invention. Evidence that claim 1 fail(s) to correspond in scope with that which applicant(s) regard as the invention can be found in the reply filed on 8/7/2006. In that paper, applicant has stated determination is made as to whether a network exploit rule in the configuration file is to be evaluated, which can lead to inefficient processing if rules are defined that are not desired to be evaluated, and this statement indicates that the invention is different from what is defined in the claim(s) because the claimed invention recites "a determination is made as to whether an intrusion protection evaluates the network exploit rule".

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international

> application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 8, 13-14, and 16 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 6,728,885 to Taylor et al.

As per claim 8: Taylor et al discloses generating a text file defining a network-exploit rule (col. 3, line 54 - col.4, line 3 and col. 6, lines 44-57). Taylor et al discloses specifying at least one field during generation of the text file such as "allow/deny" field that specifies the port to be filtered. Taylor et al also specifies a filter rule with the range of ports (priority or severity level) to be allowed or denied; and explicitly discloses a field value indicating type of filter rule to apply; therefore, the above meets the recitation of specifying at least one field selected from the group consisting of an enabled field value and a severity level field value during generation of the text file (see Col 6, lines 31-57 and Col 10, line 51 through Col 11, line 32).

As per claim 13: Taylor et al discloses a computer-readable medium having stored thereon set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of: reading input from an input device of the computer; compiling the input into a machine readable signature file comprising machine-readable logic representative of the network-exploit rule (Col 6, lines 4-12 and Col 3, line 54- Col 4, line 3 and Col 6, lines 43-57) and a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field. (Col 6, lines 31-57); evaluating the machine readable signature file and determining the value of the at least one field of the machine readable signature file (see Col 11, lines 5-67 and Col 12, lines 20-39).

As per claim 14: Taylor et al discloses specifying a threshold SEVERITY value (see Col 6, lines 1-30 and Col 10, line 51 through Col 11, line 20).

As per claim 16: Taylor et al discloses generating a text file from the input the text file specifying the network-exploit rule, the machine readable signature file compiled from the text file (col. 3, line 54 - col.4, line 3 and col. 6, lines 44-57). Taylor et al discloses specifying at least one field during generation of the text file such as "allow/deny" field that specifies the port to be filtered. Taylor et al also specifies a filter rule with the range of ports (priority or severity level) to be allowed or denied; and explicitly discloses a field value indicating type of filter rule to apply; therefore, the above meets the recitation of specifying at least one field.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-7, 9-12, 15, and 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,728,885 to Taylor et al in view of US Patent 5,987,611 to Freund.

As per claim 1: Taylor et al discloses a node of a network for managing an intrusion protection system, the node comprising: a memory module for storing data in machine-readable format for retrieval and execution by a central processing unit (Col 5, lines 10-20); and an operating system comprising a network stack comprising a protocol driver and a media access control driver and operable to execute an intrusion protection system management application (Col 4, lines 25-67), the management application operable to receive text-file input from an input device the text file defining a network exploit rule and comprising at least one field (Col 6, lines 4-12 and Col 3, lines 54-58 and Col 6, lines 43-57). Taylor et al is silent about a determination is made as to whether an intrusion protection evaluates the network exploit rule. Freund in an analogous art teaches a computer environment for monitoring access to an open network monitoring and filtering of access is provided in conjunction with a centralized enforcement supervisor and the method comprising transmitting a filtered subset of the rules to at least one other node of the network. Freund discloses that by being able to transmit filtered subset of the rules to particular computer to determine violations, the system provides many advantages such as independent monitoring and restriction of access rules for individual clients, workgroups, or entire organization (see Col 5, line 30 through Col 6, line 28 and Col 8, line 40 through Col 9, line 36). Freund discloses a machine readable signature-file database operable to store a plurality of machine-readable signature-files each generated from one of a respective plurality of text-files (see Col 21, lines 8-40). Freund discloses “enforcement of any given rule can be suspended by “disabling” the rule” (see figures 7 and column 24, lines 31-45). Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to include information determination is made as to whether an intrusion protection evaluates the network exploit rule. One of ordinary skill in the art would have been motivated to do so to benefit from the advantages disclosed above as suggested by Freund.

As per claim 2: the references as combined above disclose the claimed node of claim 1. Taylor et al discloses the limitation of a network exploit rule comprising of connection enabled field and filter to be applied that meets the recitation of wherein the network exploit rule further comprises a field selected from the group consisting of an ENABLED field and a SEVERITY field. (Col 6, lines 31-57 and Col 10, line 51 through Col 11, line 32). (See also Freud, figures 7 and column 24, lines 31-45).

As per claims 3-5, 9-10, & 15: the references as combined above disclose the claimed node of claims 1 and 2 and Taylor et al further suggests using a network comprising plurality of hosts and that the configuration file can be stored in any hosts (see Col 1, lines 15-28 and Col 4, lines 25-50) and transmitting attribute information. Although Taylor et al is silent about transmitting the machine-readable signature-file to at least one other node of the network, it is apparent that the system id configured to transmit from one host to another or one node to another. Freund in an analogous art teaches a computer environment for monitoring access to an open network monitoring and filtering of access is provided in conjunction with a centralized enforcement supervisor and the method comprising transmitting a filtered subset of the rules to at least one other node of the network (see Col 5, lines 38-43). Freund discloses that by being able to transmit filtered subset of the rules to particular computer to determine violations, the system provides many advantages such as independent monitoring and restriction of access rules for individual clients, workgroup level, or entire organization (see Col 5, line 30 through Col 6, line 28 and Col 8, line 40 through Col 9, line 36). Freund discloses transmitting a machine readable signature file to another node upon determining the severity field is greater than a threshold (see Col 28, lines 3-13 and Col 28, line 64 – Col 29, line 5). Freund discloses a machine readable signature-file database operable to store a plurality of machine-readable signature-files each generated from one of a respective plurality of text-files (see Col 21, lines 8-40). Therefore it would have been obvious to one ordinary skill in the art at the time the invention was made to include the step of transmitting a filtered subset of the rules to at least one other node of the network in order to provide independent monitoring and restriction of access rules for individual clients, workgroups, or entire organization. One of ordinary skill in the art would have been motivated to do so to benefit from the advantage disclosed above as suggested by Freund.

As per claims 6, 11, & 17: the combination of Taylor et al and Freund discloses wherein the subset of signatures comprises all machine-readable signature-files of the plurality of machine-readable signature-files each generated from a respective text-file having an asserted

ENABLED field value (see Freund Col 5, lines 40-52 and Col 21, lines 8-40). Therefore, these claims are rejected on the same rationale as the rejection of claims 3-5, 9-10, & 15 above.

As per claims 7 and 12: the combination of Taylor et al and Freund discloses wherein management application is operable to accept a SEVERITY threshold from the input device and the subset of signatures comprises all machine-readable signature-files respectively generated from a text-file having a SEVERITY field value equal to or greater than the threshold (see Freund Col 5, lines 40-52 and Col 21, lines 8-40; and Taylor et al, Col 6, lines 1-21 and Col 10, line 51 through Col 11, line 32). Therefore, these claims are rejected on the same rationale as the rejection of claims 3-5, 9-10, & 15 above.

As per claim 18: the combination of Taylor et al and Freund discloses the claimed node of claim 1 and further discloses the management application is operable to determine based at least in part on the at least one field one of a plurality of other nodes to which the network exploit rule is to be distributed (Col 28, lines 3-13 and Col 28, line 64 – Col 29, line 5). In another embodiment, Freund specifies protocols, application and application versions which are to be affected by the rule the user can conveniently encapsulate specific users, computers (or subgroups thereof) into a user-specified group that meets the recitation of the management application is operable to determine based at least in part on the at least one field one of a plurality of other nodes to which the network exploit rule is to be distributed (see Col 26, lines 31-50 and Col 25).

As per claim 19: the combination of Taylor et al and Freund discloses wherein the ENABLED field value specifies whether the network exploit-rule is enabled for evaluation by an intrusion protection system and wherein the SEVERITY field value a severity value of the network exploit-rule (Taylor et al, col. 3, line 54 - col.4, line 3 and col. 6, lines 44-57). (See also Freund, figures 7 and column 24, lines 31-45).

As per claim 20: the combination of Taylor et al and Freund discloses distributing the network exploit rule and the at least one field to a plurality of nodes (see Freund, Col 5, lines 5-45) and determining by an intrusion protection system of each of the plurality of nodes based at least in part on the at least one field whether to evaluate the network exploit rule in protecting the intrusion protection system's respective node (see Freund, figures 7 and column 24, lines 31-45). Therefore, claim 20 is rejected on the same rationale as the rejection of claims 3-5, 9-10, & 15 above.

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

5.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CC
Carl Colin
Patent Examiner
October 20, 2006

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

10/22/06